

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

Jeffrey Wan, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

DraftKings Inc.,

Defendant.

Civil Action No. 1:24-cv-09557

**FIRST AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Plaintiff Jeffrey Wan (“Plaintiff”) brings this action on behalf of themselves and all others similarly situated against DraftKings Inc. (“Defendant”). Plaintiff makes the following allegations pursuant to the investigation of Plaintiff’s counsel and based upon information and belief, except as to the allegations specifically pertaining to themselves, which are based on Plaintiff’s personal knowledge.

NATURE OF THE ACTION

1. Defendant DraftKings Inc. (“Defendant”) owns and operates its online and mobile applications (“Apps”), including casino.draftkings.com (the “Website”). Through its Website and Apps, Defendant delivers audiovisual materials, such as prerecorded videos and games containing prerecorded videos. Defendant’s website and business are tailored to serve these prerecorded videos and games containing prerecorded videos.

2. Unbeknownst to Plaintiff and the Class Members, Defendant employed Facebook, among other third parties, to intercept and disclose consumers’ search terms, video watching information, and personally identifiable information without seeking or obtaining their consent. In so doing, Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710, *et seq.* the Federal Wiretap Act (“Wiretap Act”).

JURISDICTION AND VENUE

3. This Court has original jurisdiction under 28 U.S.C. § 1331 based on Plaintiff's claims under the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.* This Court also has subject matter jurisdiction over this lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a proposed class action in which: (1) there are at least 100 Class Members; (2) the combined claims of Class Members exceed \$5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Defendant and at least one Class member are domiciled in different states.

4. This Court has personal jurisdiction over Defendant because it conducts substantial business within New York, including the sale, marketing, and advertisement of its Website and products. Furthermore, a substantial portion of the events giving rise to Plaintiff's claims occurred in this State.

5. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant resides in this District, and a substantial part of the events giving rise to Plaintiff's claims took place within this District.

PARTIES

6. Plaintiff Jeffrey Wan is a citizen of New York, who resides in New York, New York. Plaintiff Wan has created an account with Defendant, by providing Defendant their email address and first and last name, and watched a prerecorded videos on Defendant's Website within the last two years of filing of this Complaint. Throughout Plaintiff Wan's interactions with Defendant's Website, Plaintiff Wan has maintained and used Plaintiff's Facebook account from the same browser Plaintiff used to play games, which contained prerecorded audio visual content and watched prerecorded videos from Defendant's Website.

7. During that time, Plaintiff Wan (b) accessed the Website; (b) had a Facebook

profile that publicly displayed his first and last name, gender, photograph and college alma mater; (c) logged into his Facebook account; (d) searched for, clicked on, and watched pre-recorded videos on the Website; (e) clicked on various category sections to help him find games to play; and (f) clicked on games on Defendant's website, which served Plaintiff prerecorded audiovisual content upon loading the game in the form of videos, and also by clicking elements within the game.

8. Plaintiff interacted with the Website mainly in private setting. He had a reasonable expectation of privacy when using the Website and Apps. He did not have the expectation that third parties like Facebook were intimately tracking him or involved in his interactions with the Website and Apps.

9. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language and country – are “always public.”¹ No privacy setting on a Facebook account would allow Plaintiff, or any users, to hide this basic information.

10. Pursuant to the systematic process described herein, Defendant caused Plaintiff Wans's video viewing habits to be sent along with Plaintiff's personally identifiable information (“PII”) and other persistent cookies and trackers (including his IP address) to Facebook and upon information and belief, other third parties (collectively, the “Tracking Entities”) without Plaintiff's knowledge or consent each time Plaintiff requested and viewed a game or video content through the Website.

11. Plaintiff Wan never consented, agreed, nor permitted Defendant to disclose Plaintiff's PII and viewing information to Facebook or other third parties and certainly did not do

¹ *Control who can see what you share on Facebook*, FACEBOOK, <https://www.facebook.com/help/1297502253597210> (last visited March 13, 2025).

so for purposes violative of the VPPA and Wiretap Act.

12. Defendant DraftKings Inc. is a Nevada corporation with its principal place of business located in Boston, Massachusetts.

GENERAL ALLEGATIONS

A. History and Overview of the VPPA

13. The impetus for the VPPA began with President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a movie rental store disclosed the nominee's rental history to the Washington City Paper which then published that record. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator Patrick Leahy, who introduced the Act, explained:

"It is nobody's business what Oliver North or Pratik Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong".

S. Rep. 100-599, at 5-6 (internal ellipses and brackets omitted).

14. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

15. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). The VPPA defines personally identifiable information ("PII") as "information which identifies a person as having requested or obtained specific video materials

or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3). A video tape service provider is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

B. The VPPA and Video Games

16. The VPPA covers “prerecorded video cassette tapes or similar audio visual materials,” see 18 U.S.C. § 2710(a)(4), and Congress intended that to include materials like “laser discs, open-reel movies, or CDI technology[.]” *See* S. Rep. 100-599.

17. In 1986, “Philips and Sony announced that they were developing standards for a new medium based on the CD and CD-ROM technology.”² This new format, known as Compact-Disc Interactive, or CD-I, promised to “make it possible to store audio, video, text, computer-generated images, or any combination of these on a compact disc.”³

18. In 1991, that vision turned into reality. Philips introduced a new console, the Philips CDI 910, which “play[ed] cinema-quality computer games, educational programs, movies, and other multimedia products that combine video, audio and text features in an interactive rather than a play-only mode.”⁴ The new console played games like “Voyeur,” for example, which was “a kind of high-tech version of Clue[.]” allowing users to “make decisions for characters and even change the outcome of the mystery.”⁵

² *See* Scott A. Stewart, *Videodiscs in Healthcare: A Guide to the Industry*, THE MEDICALDISC REPORTER (1990), *archived at* <https://tinyurl.com/44ypcaht>.

³ *See* ENCYCLOPEDIA OF LIBRARY AND INFORMATION SCIENCE 98 (1992), *archived at* <https://tinyurl.com/mt2vutat>.

⁴ Patrick Oster, Philips’s *Multimedia Makeover; Dutch Electronics Firm Escapes Crisis, but Can It Compete Globally?*, WASH. PO. (Oct. 26, 1994), *archived at* <https://tinyurl.com/4xwnausj>.

⁵ David Elrich, *Interactive Video: Armchair Activities*, N.Y. TIMES (Dec. 9, 1993), *archived at* <https://nyti.ms/3Wp2wkZ>.

19. The Philips CDI 910 was initially a joint project between Philips and Sony, but “mounting conflicts resulted in a parting of ways.”⁶ That would prove advantageous for Sony. The Philips CDI 910 ultimately underperformed, receiving only a lukewarm response from consumers, but “its arrival cemented the CD-ROM as a medium for entertainment beyond the computer[,]”⁷ and that same year, Sony unveiled its own console, the “Play Station,” which used a CD-ROM drive to “play videogames as well as other forms of interactive entertainment, as was considered important at the time.”⁸

20. Even before CD-I and CD-ROM, however, laser discs were used for video games and other interactive content. As early as 1981, laser discs “permit[ted] the viewer to not only manipulate the programming, but to interact with the material – play games, take quizzes, adjust pacing and repeat sections as desired.”⁹ During that same period, VHS tapes could also contain interactive content, like the television series “Captain Power and the Soldiers of the Future,” which used “video game technology” to create an interactive experience, emitting “a signal, encoded in the television film, that both activates and responds to light rays emitted by the toy – a jet aircraft with a pistol grip – when the user pulls the trigger.”¹⁰

21. These technologies blurred the line between video games and movies. As one commentator noted, “more and more movies look and sound like video games, and now that more and more video games look and sound like movies, it seems possible that the new art form might well swallow up the old.”¹¹ By 1982, video games were distributed “in the record and

⁶ IGN Staff, *History of the PlayStation: The greatest story ever told*, IGN (Jun. 21, 2012), available at <https://tinyurl.com/25245e9t>.

⁷ *Id.*

⁸ *Id.*

⁹ Myron Berger, *High-Tech Equipment Comes of Age*, N.Y. TIMES (Sept. 27, 1981), archived at <https://tinyurl.com/bnt57hvy>.

¹⁰ Sandra Salmans, *The Interactive World of Toys and Television*, N.Y. TIMES (Oct. 4, 1987).

¹¹ Vincent Canby, *Are Video Games About to Zap the Action Movie*, N.Y. TIMES (May 15, 1983), archived at <https://tinyurl.com/5fv5s6v3>.

video stores[,]”¹² and by 1983, 400 games were in circulation, “including several controversial X-rated games and a game based on the television series ‘M-A-S-H,’ in which the uplifting goal is to take the most wounded soldier to a hospital.”¹³

22. The evolution of interactive content from laser discs and VHS tapes to modern digital platforms has pushed the boundaries of gaming platforms. Today, video games include the same audio-visual materials found in traditional laser discs and VHS tapes that the VPPA seeks to protect.

C. History and Overview of the Federal Wiretap Act

23. Congress enacted The Federal Wiretap Act “as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications.”¹⁴

24. The Wiretap Act primarily concerned the government’s use of wiretaps but was amended in 1986 through the Electronic Communications Privacy Act (“ECPA”) to provide a private right of action for private intrusions as though they were government intrusions.¹⁵

25. Congress was concerned that technological advancements like “large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing”¹⁶ were rendering the Wiretap Act out-of-date. Congress amended the Wiretap Act in 1986 through the Electronic Communications Privacy Act (“ECPA”) to provide a private right of action for private intrusions as though they were

¹² Aljean Harmetz, *Hollywood Discovering Video Games*, N.Y. TIMES (July 1, 1982), *archived at* <https://tinyurl.com/mvcaswf2>.

¹³ Aljean Harmetz, *Makers Vie for Millions In Home Video Games*, N.Y. TIMES (Jan. 13, 1983), *archived at* <https://tinyurl.com/5n84ccc3>.

¹⁴ Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act’s Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022), <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1541&context=crsj>

¹⁵ *Id.*

¹⁶ Senate Rep. No. 99-541, at 2 (1986).

government intrusions.

26. As a result, the ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third-party processing of data and files. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

27. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

28. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not “intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. §2511(2)(d).

D. Defendant’s Website and Tracking Tools

a. Overview of How Websites Operate

29. When companies like Defendant build their websites, they install or integrate various third-party scripts into the code the website to collect data from users or perform other functions.¹⁷

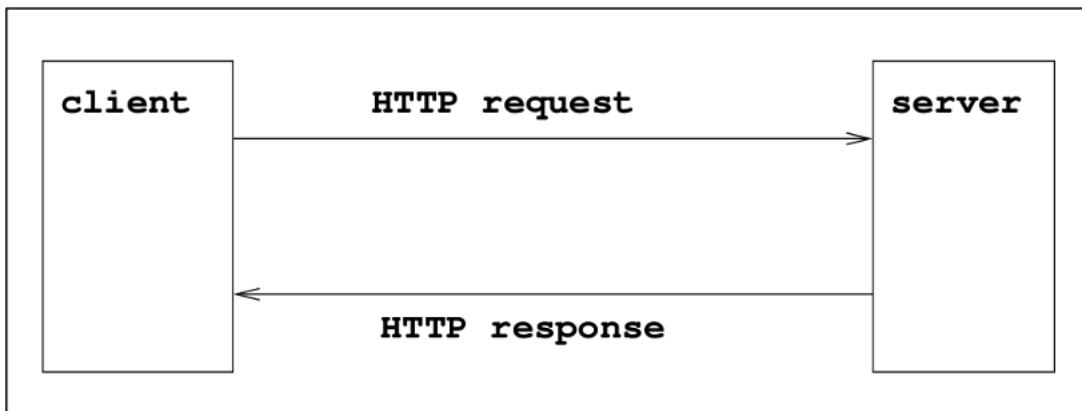
30. Oftentimes, third-party scripts are installed on websites “for advertising

¹⁷ See *Third-party Tracking*, PIWIK, <https://piwik.pro/glossary/third-party-tracking/> (“Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user’s visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user’s browsing history to other companies...”).

purposes.”¹⁸ Further, “[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time.”

31. To make Defendant’s Website load on a user’s internet browser, the browser sends an “HTTP request” or “GET” request to Defendant’s server where the relevant Website data is stored. In response to the request, Defendant’s server sends an “HTTP response” back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant’s Website transmits instructions back to users’ browsers in response to HTTP requests. (See Figure 1.)

Figure 1:



32. The server’s instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what videos should play.

33. When a user navigates to a webpage (by entering a URL address directly or clicking a hyperlink containing the address), that user’s browser contacts the DNS (Domain Name System) server, which translates the web address of that website into a unique IP (Internet Protocol) address.

¹⁸ *Id.*

34. An IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

35. When a user's browser navigates to a webpage, it sends an HTTP request to the server identified by the webpage's IP address. This request is for the specific resource located at the URL. If the server fulfills this request, it issues an HTTP response, which includes the status of the request and, typically, the requested content. This content is then transmitted in small chunks, known as data packets, and reassembled into the complete webpage upon arrival by the user's browser.¹⁹

36. This request URL includes a domain name and path, which identify the specific content being accessed on a website and its location within the website's structure.

37. The request URL typically contains parameters. Parameters are values added to a URL to transmit data to the recipient, prefaced by a question mark to signal the use of parameters. Parameters direct a web server to provide additional context-sensitive services. (See Figure 2.)

38. Defendant has implemented a myriad of sophisticated tracking tools that operate

Figure 2:



covertly when users access and navigate its Website, including Facebook, and upon information

¹⁹ *What is an IP Address – Definition and Explanation*, KASPERSKY, <https://usa.kaspersky.com/resource-center/definitions/what-is-an-ip-address> (last accessed January 30, 2025).

and belief, TikTok, and Hotjar. The Tracking Parties use a myriad of cookies and other persistent trackers (collectively, the “Tracking Tools”) to capture a user’s IP address and long-string URLs revealing a host of information about that user’s private activities on the Website, as explained at greater depth below.

b. The Facebook Tracking Pixel

39. Facebook is the largest social networking site on the planet, touting 2.9 billion monthly active users.²⁰ Facebook describes itself as a “real identity platform,”²¹ meaning users are allowed only one account and must share “the name they go by in everyday life.”²² To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.²³

40. Facebook generates revenue by selling advertising space on its website.²⁴

41. Facebook sells advertising space by highlighting its ability to target users.²⁵ Facebook can target users so effectively because it surveils user activity both on and off its site.²⁶ This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”²⁷ Facebook compiles this information into a generalized dataset called “Core Audiences,” which businesses use to apply highly specific

²⁰ Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, YAHOO (July 28, 2021), <https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267>.

²¹ Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

²² FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

²³ FACEBOOK, SIGN UP, <https://www.facebook.com/>

²⁴ Mike Isaac, *Facebook’s profit surges 101 percent on strong ad sales.*, N.Y. TIMES (July 28, 2021), <https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html>.

²⁵ FACEBOOK, WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706>.

²⁶ FACEBOOK, ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

²⁷ FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

filters and parameters for their targeted advertisements.²⁸

42. Businesses that advertise can also build “Custom Audiences.”²⁹ Custom Audiences enable businesses to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”³⁰ Businesses can use a Custom Audience to target existing customers directly, or they can use it to build a “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”³¹ Unlike Core Audiences, Custom Audiences require an advertiser to supply the underlying data to Facebook. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools,” which collect and transmit the data automatically.³² One such Business Tool is the Facebook Tracking Pixel.

43. The Facebook Tracking Pixel is a piece of code that businesses, like Defendant, can integrate into their website. Once activated, the Facebook Tracking Pixel “tracks the people and type of actions they take.”³³ When the Facebook Tracking Pixel captures an action, it sends a record to Facebook. Once this record is received, Facebook processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences.

²⁸ FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences>.

²⁹ FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

³⁰ FACEBOOK, ABOUT EVENTS CUSTOM AUDIENCE, <https://www.facebook.com/business/help/366151833804507?id=300360584271273>.

³¹ FACEBOOK, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

³² FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

³³ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

44. Businesses control what actions—or, as Facebook calls it, “events”—the Facebook Tracking Pixel will collect, including the website’s metadata, along with what pages a visitor views.³⁴ Business can also configure the Facebook Tracking Pixel to track other events. Facebook offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases.³⁵ A business can also create their own tracking parameters by building a “custom event.”³⁶

45. Businesses control how the Facebook Tracking Pixel identifies visitors. The Facebook Tracking Pixel is configured to automatically collect “HTTP Headers” and “Pixel-specific Data.”³⁷ HTTP Headers collect “IP addresses, information about the web browser, page location, document, referrer and persons using the website.”³⁸ Pixel-specific Data includes “the Pixel ID and cookie.”³⁹

46. The Facebook Tracking Pixel also allows advertisers “to track [its] website visitors’ actions,” which Meta calls conversion tracking.⁴⁰ “Tracked conversions ... can be used to analyze [Defendant’s] return on ad investment.”⁴¹ Notably, “[e]ach time the Pixel loads, it automatically ... track[s]” and records the URL that a website user viewed.⁴² In other words, so

³⁴ See FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP,

<https://www.facebook.com/business/help/218844828315224?id=1205376682832142>.

³⁵ FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

³⁶ FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>.

³⁷ FACEBOOK, FACEBOOK PIXEL, <https://developers.facebook.com/docs/facebook-pixel/>.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ FACEBOOK, CONVERSION TRACKING, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking>.

⁴¹ *Id.*

⁴² FACEBOOK, CUSTOM CONVERSIONS,, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

long as an advertiser has installed the Facebook Tracking Pixel on their website, anyone who views that webpage—meaning all website users—“will be tracked using that” automatic URL tracker.⁴³ And, as mentioned above, the tracked URL discloses to Facebook the exact video(s) that a website user views. Indeed, Facebook even warns advertisers to “make sure” the website URLs are specific enough so advertisers “can define visitor actions exclusively based on unique ... website URLs.”⁴⁴

47. “Once tracked, custom conversions”—such as the URL tracking tool—“can be used to optimize [] ad campaigns”⁴⁵ through other Facebook tools such as Ads Insights.⁴⁶ Notably, this part of Facebook’s functionality ignores users’ decision to opt out of tracking, collecting the same data it would otherwise through “a connection between an advertiser’s server and Meta’s Conversion API endpoint.”⁴⁷

48. After receiving information from businesses like Defendant, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

49. Facebook confirms, in its “Meta Business Tools Terms,”⁴⁸ that it has the capability to use the information it collects for purposes other than recording it and conveying it to advertisers. For instance, Facebook can use the information it collects “to promote safety and security on and off the Meta Products, for research and development purposes and to maintain the integrity of and to provide and improve the Meta Products.”⁴⁹ In other words, Facebook can use the wiretapped information for its own “research and development,” and to “protect” its own

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ FACEBOOK, CUSTOM CONVERSIONS INSIGHTS, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking#custom-conversions>.

⁴⁷ *Id.*

⁴⁸ FACEBOOK, META BUSINESS TOOLS TERMS, <https://m.facebook.com/legal/businesstech>.

⁴⁹ *Id.*

products and services.⁵⁰

50. Facebook can also connect all information it collects to analyze and generate reports regarding advertising campaigns, create custom audience sets that can be shared with other advertisers, and “use your Event Data for ads delivery only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Meta Products.”⁵¹

51. Further, Facebook can use the event data to help websites “reach people with transactional and other commercial messages on [Facebook] Messenger and other Meta Products.”⁵²

52. At all relevant times herein, Defendant’s Website hosts and/or has hosted the Facebook Tracking Pixel and other Facebook tracking tools—including the URL trackers—described above.

53. More specifically, the Facebook Pixel that Defendant installed and used tracked, recorded, and sent Facebook its subscribers’ granular Website and apps activity, including the names of specific prerecorded videos and games that subscribers requested and/or viewed each time through Defendant’s Website and apps. The information is not merely metadata.

54. Defendant’s motivation for using the Facebook Tracking Pixel and related Facebook Business Tools is simple—it financially benefits Defendant in the form of advertising and information services that Defendant would otherwise have to pay for.

55. The information Facebook receives from Defendant identifies subscribers based on their unique and persistent Facebook IDs (“FID”), which is sent to Facebook as one data point alongside the title of the video content the specific subscriber requested or viewed. Defendant’s use of the Facebook Tracking Pixel is depicted below. The term “PageView” discloses a video’s

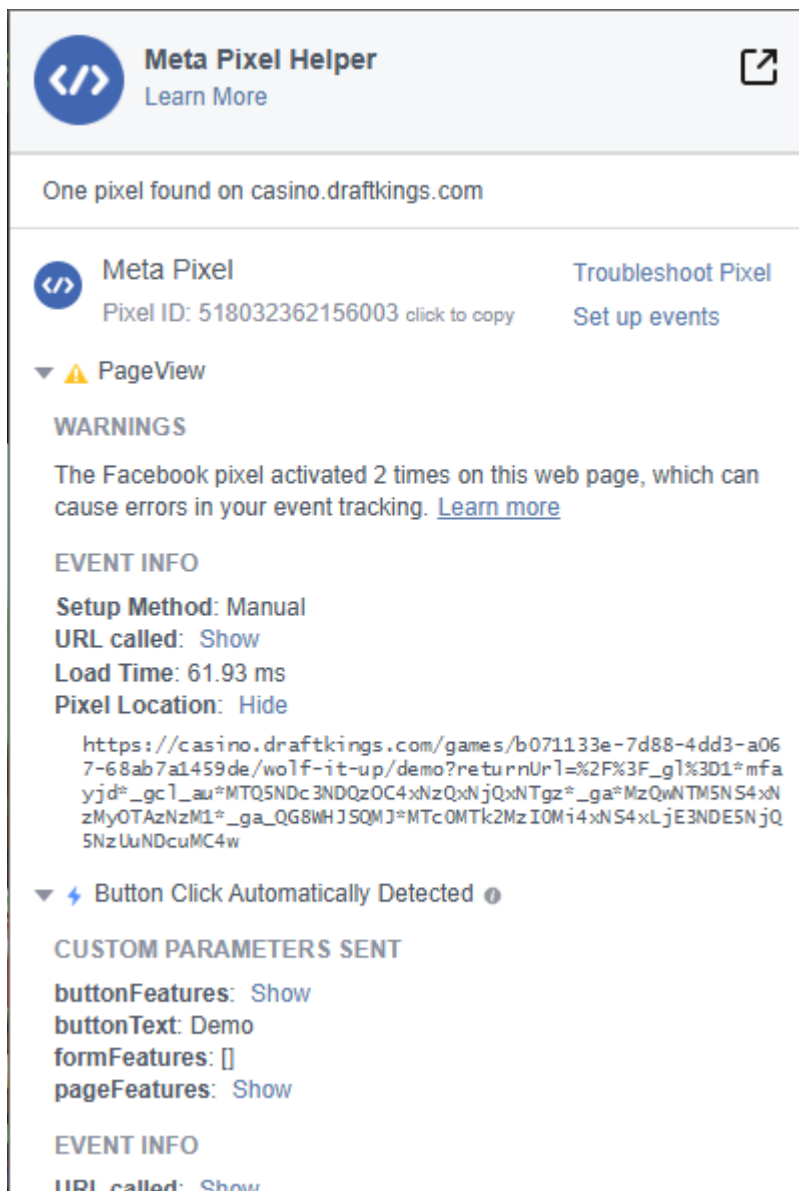
⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

URL whenever a viewer accesses that webpage.

Figure 1:

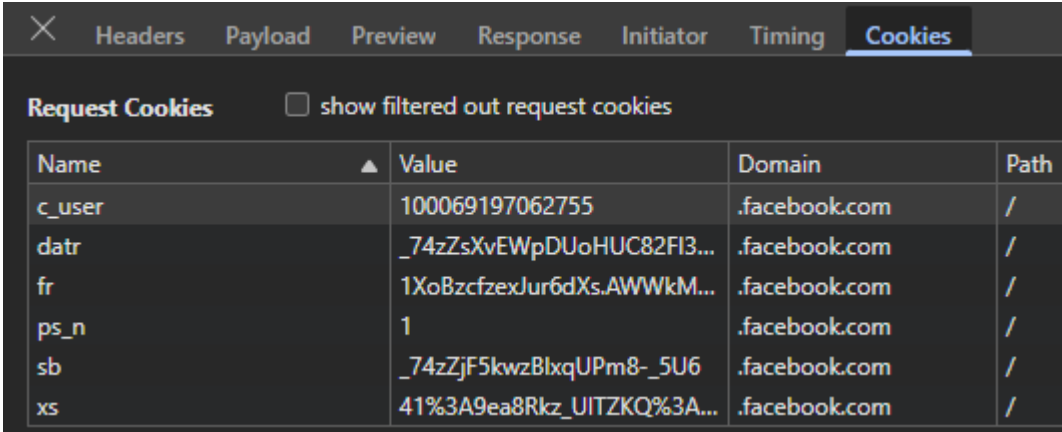


56. Defendant's use of the Facebook Tracking Pixel permits an ordinary person to identify a video's content, title, and URL.

57. When a visitor watches a video or plays a game on the Website while logged into Facebook, Defendant compels a visitor's browser to transmit the c_user cookie to Facebook. The c_user cookie contains that visitor's unencrypted Facebook ID. When accessing the above game,

for example, Defendant compelled the browser to send six cookies:

Figure 2:



Name	Value	Domain	Path
c_user	100069197062755	.facebook.com	/
datr	_74zZsXvEWpDUoHUC82FI3...	.facebook.com	/
fr	1XoBzcfzexJur6dXs.AWWkM...	.facebook.com	/
ps_n	1	.facebook.com	/
sb	_74zZjF5kwzBlxqUPm8-_5U6	.facebook.com	/
xs	41%3A9ea8Rkz_UITZKQ%3A...	.facebook.com	/

58. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.⁵³ The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser.⁵⁴ The datr cookies also identifies a browser.⁵⁵ Facebook, at a minimum, uses the fr and _fbp cookies to identify users.⁵⁶

59. Without a corresponding Facebook ID, the fr cookie contains, at least, an abbreviated and encrypted value that identifies the browser. The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser. Facebook uses both for targeted advertising.

60. The fr cookie will expire after 90 days unless the visitor's browser logs back into Facebook. If that happens, the time resets, and another 90 days begins to accrue.⁵⁷

61. The fr cookie will expire after 90 days unless the visitor's browser logs back into

⁵³ DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

⁵⁴ FACEBOOK, CONVERSION API, <https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/>.

⁵⁵ FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

⁵⁶ *Id.*

⁵⁷ Also confirmable through developer tools.

Facebook.⁵⁸ If that happens, the time resets, and another 90 days begins to accrue.⁵⁹

62. The Facebook Tracking Pixel uses both first- and third-party cookies. A first party cookie is “created by the website the user is visiting”—*i.e.*, DraftKings.⁶⁰ A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—*i.e.*, Facebook.⁶¹ The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

63. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to Facebook IDs and corresponding Facebook profiles.

64. A Facebook ID is personally identifiable information. Anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of Facebook.com.

65. Through the Facebook Tracking Pixel’s code, these cookies combine the identifiers with the event data, allowing Facebook to know, among other things, what DraftKings videos a user has watched or game played.⁶²

66. Defendant also chose to use “Automatic Advanced Matching.” When activated, the Facebook Tracking Pixel “look[s] for recognizable form field and other sources on your website that contain information such as first name, last name and email.”⁶³ The Facebook Tracking Pixel’s code collect[s] that information, “along with the event, or action, that took

⁵⁸ *Id.*

⁵⁹ Confirmable through developer tools.

⁶⁰ PC MAG, *FIRST-PARTY COOKIES*, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>. This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

⁶¹ *Id.*

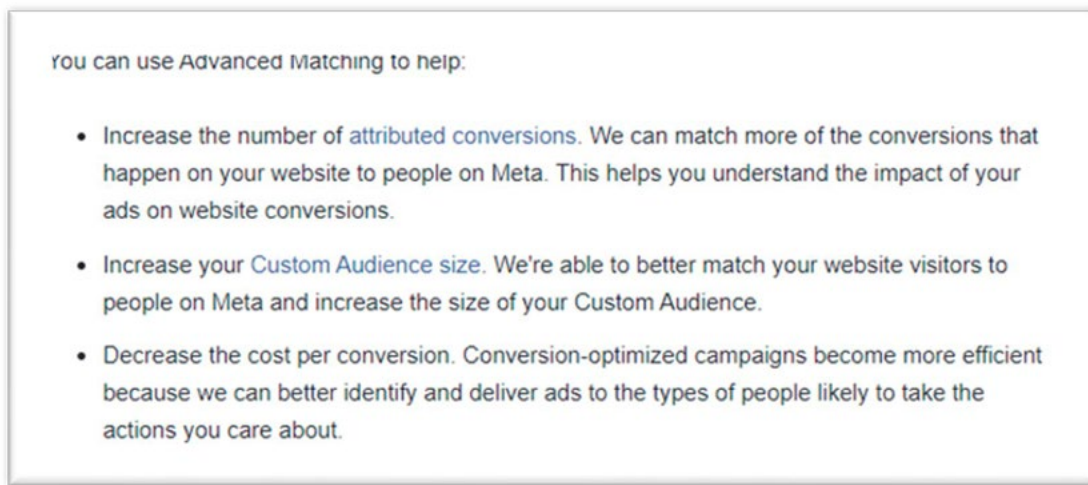
⁶² *Id.*

⁶³ FACEBOOK, GET STARTED, <https://developers.facebook.com/docs/meta-pixel/get-started>.
38 <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>

place.”⁶⁴ This information is “hashed,”⁶⁵ meaning it is “[a] computed summary of digital data that is a one-way process.”⁶⁶ In other words, it “cannot be reversed back into the original data.”⁶⁷

67. DraftKings discloses this information so it can better match visitors to their Facebook profiles, which thereby allows DraftKings to better track analytics and target its advertisements:

Figure 3:



68. DraftKing’s Facebook Tracking Pixel is configured to scan form fields containing a user’s email, first name, last name, gender, phone number, city, state, and zip code:⁶⁸

Figure 4:

⁶⁴ FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB, <https://www.facebook.com/business/help/611774685654668?id=1205376682832142>.

⁶⁵ DEFINITION OF HASH, <https://www.pcmag.com/encyclopedia/term/hash>

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Facebook provides a corresponding look-up table: FACEBOOK, ADVANCED MATCHING, <https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching>.


```
f.ensureModuleRegistered("SignalsPixelPIIConstants", function() {
  return function(g, h, i, j) {
    var k = {
      exports: {}
    };
    k.exports;
    (function() {
      "use strict";
      var a = f.getFbeventsModules("SignalsFBEventsUtils")
        , b = a.keys;
      a = a.map;
      var c = {
        ct: "ct",
        city: "ct",
        dob: "db",
        dobd: "dobd",
        dobm: "dobm",
        doby: "doby",
        email: "em",
        fn: "fn",
        f_name: "fn",
        gen: "ge",
        ln: "ln",
        l_name: "ln",
        phone: "ph",
        st: "st",
        state: "st",
        zip: "zp",
        zip_code: "zp"
      };
    })();
  };
});
```

69. DraftKings knows Facebook will match the Advanced Matching parameters with a subscriber's subsequent activity, thereby helping DraftKings "[i]ncrease the number of attributed conversions," "[i]ncrease [its] Custom Audience size," and "[d]ecrease the cost per conversion."⁶⁹

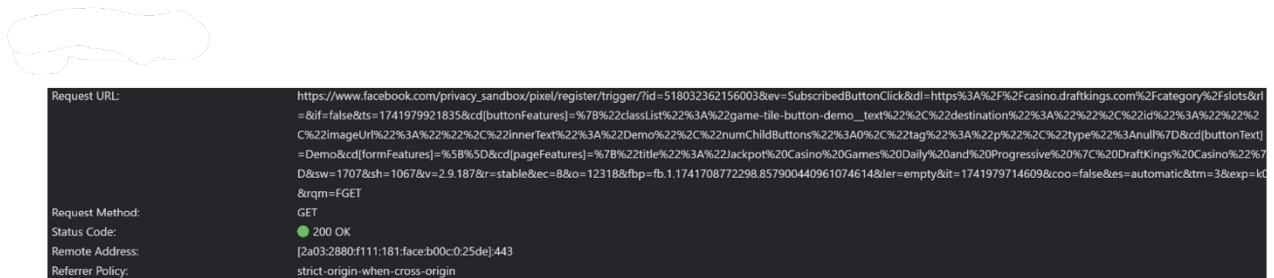
70. In addition to capturing and sharing its subscribers PII and irrespective of how the they reached the web watching page, through its URL tracking technology, DraftKings also intercepted and shared button clicks revealing the exact subpages (including the category of

⁶⁹ FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB,
<https://www.facebook.com/business/help/611774685654668?id=1205376682832142>.

games) that a subscriber navigates through to find the games.

71. For example, if a subscriber narrows DraftKings video game offerings to “slots,” and the clicks on the “Wolf it Up” game displayed within that category, the Facebook Tracking Pixel captures that the subscriber clicked on those buttons before arriving at the resulting webpage, as depicted below:

Figure 5:



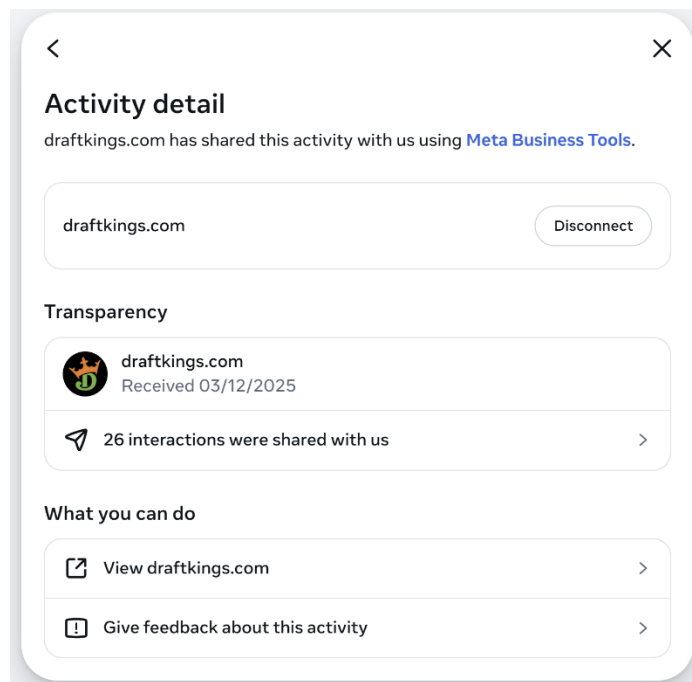
72. A breakdown of the above long-string URL reveals the trove of detailed information which DraftKings transmits to Facebook about its subscribers' private interactions within the Website. Specifically, the URL contains: (1) **Page URL**: That the event occurred on <https://casino.draftkings.com/category/slots>; (2) **Event Type**: “SubscribedButtonClick” - A custom event name for tracking when users click the “Demo” button of a game; (3) **Button Properties**: The clicked button had the class “game-tile-button-demo__text” and displayed the text “Demo”; and (4) **Page Information**: The page title was “Jackpot Casino Games Daily and Progressive | DraftKings Casino”

73. Aside from capturing its subscribers’ private communications within the Website, capturing and sharing these navigation events through Facebook’s URL trackers also discloses a subscriber’s non-public and sensitive gambling interests (e.g., “jackpot” and “slots”).

74. Facebook confirms that it matches activity on DraftKings with a user’s profile. Facebook allows users to download their “off-site activity,” which is a “summary of activity that

businesses and organizations share with us about your interactions, such as visiting their apps or websites.”⁷⁰ Here, the off-site activity report confirms DraftKings identifies an individual’s video viewing activities:

Figure 6:



75. The Facebook Pixel ID is a numerical code that uniquely identifies each Pixel.⁷¹ In practice, this means DraftKing’s Facebook Tracking Pixel has a Pixel ID that differs from all other websites. All subscribers who view video games and other videos on Defendant’s Website can pull their off-site activity report and see the same Pixel ID.

⁷⁰ FACEBOOK, WHAT IS OFF-FACEBOOK ACTIVITY?, <https://www.facebook.com/help/2207256696182627>. As discussed there, the Off-Facebook Activity is only a “summary” and Facebook acknowledges “receiv[ing] more details and activity than what appears in your Facebook activity.” What is more, it omits “information we’ve received when you’re not logged in Facebook, or when we can’t confirm that you’ve previously used Facebook on that device.”

⁷¹ FACEBOOK, GET STARTED, <https://developers.facebook.com/docs/meta-pixel/get-started>.

E. Defendant Intentionally and Knowingly Discloses its Subscribers PII in Violation of the VPPA

76. Pursuant to the systematic process detailed above, Defendant's use of the Trackers violate the VPPA and Wiretap Act.

a. Defendant is a Video Tape Service Provider

77. Defendant operates an online casino through its Website. Through its Website, it offers a plethora of prerecorded audio visual content in the form of: (a) a catalog of games containing prerecorded audio visual clips; and separately (b) prerecorded videos pertaining to various casino games.

78. The games on Defendant's website are mostly rudimentary turned-based games. They are essentially a string of prerecorded videos clips with sound that get activated sequentially based on a user's selections.

79. Thus a key element of Defendant's business model is to serve prerecorded audio visual content along with its games.

80. For many games offered by Defendant, when a user selects and opens the page for that game, the game automatically presents a prerecorded video clip with sound which is unique to that game. So at a minimum, by revealing the game the user clicked on or requested, the prerecorded video they watched as part of that game is also revealed.

81. Also, often times when a user makes a certain button clicks during the games, additional prerecorded video clips and sound play that move the game along. This prerecorded audio visual content is created and hosted by Defendant and is integral to Defendant's business.

82. Defendant specifically creates, hosts and delivers these prerecorded videos and sound to attract users and keep them hooked onto Defendant's website. Defendant's website is tailored to provide this prerecorded audio visual content to users like Plaintiff.

83. The prerecorded videos in the games are typically downloaded to the users' browsers upon engaging with the game.

84. Defendant has consumers, in the form of individuals who created an account with Defendant's Website and at a minimum provided their IP address, email address, and first and last name and/or made a purchase from Defendant's store. Moreover, consumers may pay money to Defendant to gamble on the games offered by Defendant.

b. Defendant Knowingly Discloses Consumers' PII To Third Parties

85. When customers request, view or purchase audiovisual content from Defendant's Website or Apps, their Personal Viewing Information is transmitted to Facebook, and other unauthorized third parties as a result of the tracking tools that Defendant purposely installed and implemented on its Website and Apps.

86. Defendant controlled its Website, Apps, and all of the tracking technologies that it used to transmit its customers' Personal Viewing Information to unauthorized parties. Importantly, Facebook would not have received Plaintiff's or the Class Members' Personal Viewing Information but for Defendant's decision to install and use Facebook's Business Tools, including the Facebook Pixel and Conversions API,⁷² and other tracking technologies on its Website and Apps.

87. Moreover, Defendant controlled which data was tracked, recorded, and transmitted when its customers requested or viewed its video content.

88. The information transmitted is especially sensitive because a person's interest in gambling content may negatively impact them if exposed, because casino gambling is often

⁷² Notably, the Facebook Pixel works in conjunction with its Conversion API tool and, as a result, Defendant transmits one copy of its consumer's viewing information directly from its web server to Meta's web servers. Additional copies of this information are also communicated through the use of cookies.

looked down upon in society.

89. Defendant's knowledge as to its conduct is evidenced by the fact that: (1) it chose to track its customers' interactions with the Website and Apps, including their viewing of the prerecorded videos and audio visual materials contained in games; (2) it requested and installed lines of code that achieved this purpose; (3) it obtained the lines of code from Facebook and other third parties in order to achieve this purpose; and (4) it controlled the information that was tracked, recorded, and transmitted via the Website and the Apps.

c. Defendant's use of Facebook Business Tools and Tracking Pixels

90. Notably, these marketing tools are not required for Defendant's Website or Apps to function properly. Even if it finds the tools helpful, Defendant could have used them in a manner that does not reveal its customers' Personal Viewing Information.

91. Any ordinary person who comes into possession of a Facebook ID can easily use that information to identify a particular individual and their corresponding Facebook profile, which contains additional information such as the user's name, gender, birthday, place of residence, career, educational history, a multitude of photos, and the content of a Facebook user's posts. This information may reveal even more sensitive personal information—for instance, posted photos may disclose the identity of family members, and written posts may disclose religious preferences, political affiliations, personal interests, and more.

d. Defendant's Use of Tracking Tools to Reveal Video Viewing Data

92. When Defendant's customers purchase, request or view audio visual content on Defendant's Website, the specific title of the video or game is transmitted to Facebook alongside the customers' persistent and unique Facebook identifiers, thereby revealing their Personal Viewing Information to Facebook. However, customers are unaware of this because, amongst other things, Defendant's transmissions are completely invisible to ordinary customers viewing

Defendant's webpages.

93. While Figure 1 and 3 show what ordinary customers see on their screens as they use the Website, Figures 2 and 4 shows how Defendant sends to Facebook Plaintiff and the Class Members PII along with the title of the game or video a customer requested or viewed through the Website.

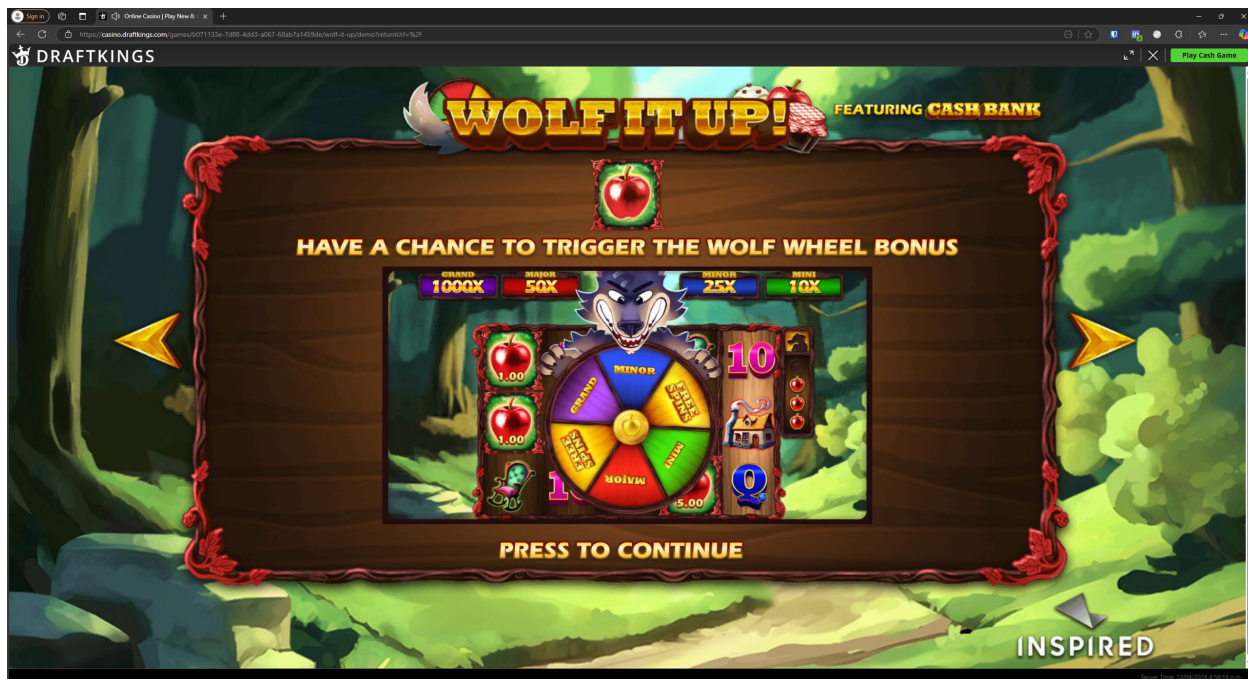


Figure 1. The image above is a screenshot of what a consumer sees when they attempt to play a game on Defendant's Website. For this specific game, called "Wolf It Up!", like many others on Defendant's website which Plaintiff has played, simply opening the page automatically plays music and prerecorded video content, even before the users does anything. The screenshot is a still from video that auto plays upon opening the game. The page does not contain any logos or indications that their interactions are recorded and sent to Facebook.

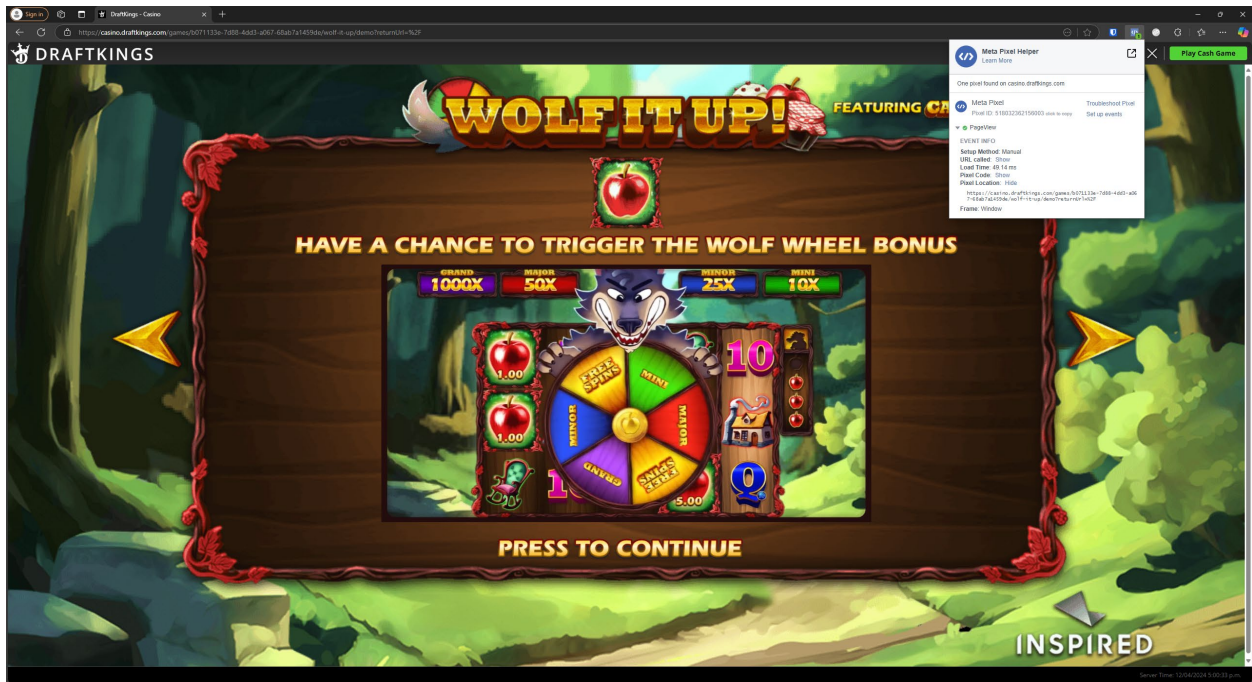


Figure 2. The images above represent a screenshot of a network traffic report that was taken when a customer attempted to play a game on Defendant's Website, at which time the personal viewing information was transmitted to Facebook.

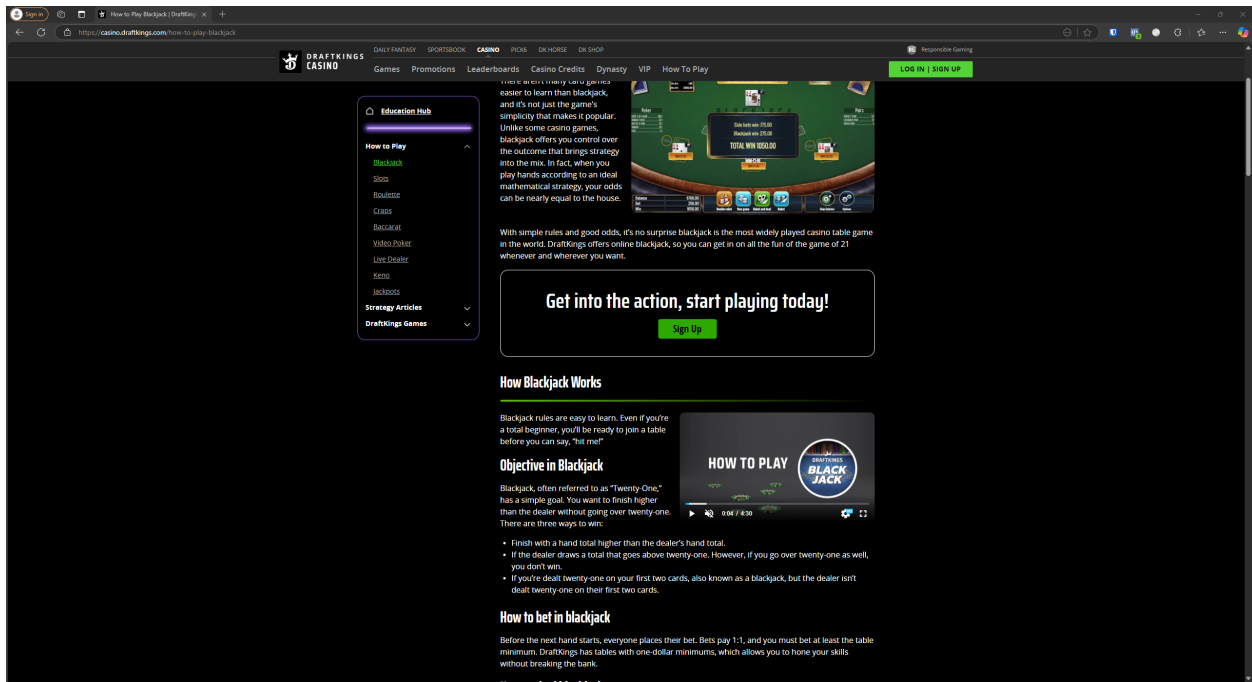


Figure 3. The image above is a screenshot of what a consumer sees when they attempt to watch a prerecorded video on Defendant's Website. The page does not contain any logos or indications that their interactions are recorded and sent to Facebook. The video auto plays on the webpage.

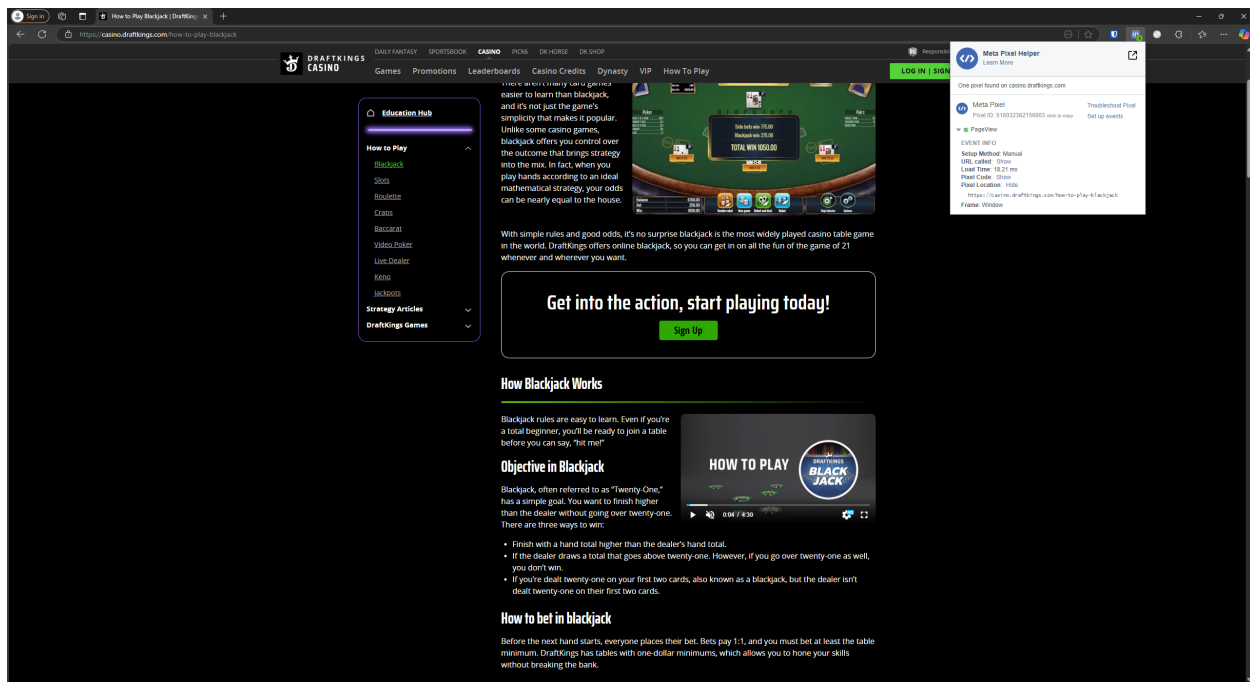


Figure 4. The images above represent a screenshot of a network traffic report that was taken when a customer attempted to watch a prerecorded video on Defendant's Website, at which time the personal viewing information was transmitted to Facebook.

94. Upon information and belief, Defendant also transmits its customers' Personal Viewing Information to Facebook and other additional unauthorized third parties – including Google, TikTok and Twitter – through other tracking technologies installed on its Website and Apps.

95. The Personal Viewing Information that Defendant obtained from Plaintiff and the Class Members is valuable data in the digital advertising-related market for consumer information.

96. At no point did Plaintiff or the Class Members consent to Defendant's disclosure of their video viewing history to third parties. As such, Defendant deprived Plaintiff and the Class Members of their privacy rights and control over their personal information.

97. The harms described above are aggravated by Defendant's continued retention and commercial use of Plaintiff's and the Class Members' personal information, including their private video viewing histories.

TOLLING

98. The statutes of limitations applicable to Plaintiff's and the Class Members' claims were tolled by Defendant's conduct and Plaintiff's and the Class Members' delayed discovery of their claims.

99. As alleged above, Plaintiff and the Class Members did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiff and the Class Members could not have discovered Defendant's unlawful conduct with reasonable diligence.

100. Defendant secretly incorporated the Tracking Tools into the Website, providing no indication to consumers that their communications would be disclosed to these third parties.

101. Defendant had exclusive and superior knowledge that the Tracking Entities' Tracking Tools incorporated on its Website would disclose consumers' protected and private information and confidential communications, yet failed to disclose that by interacting with the Website, Plaintiff's and Class Members' PII would be disclosed to third parties.

102. Plaintiff and the Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the Tracking Entities' Tracking Tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website user that Defendant was disclosing and allowing the interception of such information to these third parties.

103. The earliest that Plaintiff and the Class and Members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing this Amended Complaint.

CLASS ACTION ALLEGATIONS

104. Plaintiff brings this action on behalf of themselves and all other similarly situated

persons pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), and (b)(3).

105. Specifically, the Class is defined as:

All persons in the United States who, during the maximum period of time permitted by law, used Defendant's Website or Apps to view or request game or prerecorded video using their mobile or computer browsers.

106. The Class does not include (1) Defendant, its officers, and/or its directors; or (2) the Judge to whom this case is assigned and the Judge's staff.

107. Plaintiff reserves the right to amend the above class definition and add additional classes and subclasses as appropriate based on investigation, discovery, and the specific theories of liability.

108. ***Community of Interest:*** There is a well-defined community of interest among members of the Class, and the disposition of the claims of these members of the Class in a single action will provide substantial benefits to all parties and to the Court.

109. ***Numerosity:*** While the exact number of members of the Class is unknown to Plaintiff at this time and can only be determined by appropriate discovery, upon information and belief, members of the Class number in the millions. Members of the Class may also be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

110. ***Existence and predominance of common questions of law and fact:*** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individuals of the Class. These common legal and factual questions include, but are not limited to:

- (a) Whether Defendant collected Plaintiff's and the Class Members' PII;
- (b) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the VPPA;

(c) Whether Defendant unlawfully disclosed and continues to disclose its users' PII, including their video viewing records, in violation of the Wiretap Act;

(d) Whether Defendant's disclosures were committed knowingly; and

(e) Whether Defendant disclosed Plaintiff's and the Class Members' PII without consent and

(f) Whether Plaintiffs are the Class Members are entitled to actual and/or statutory damages for the aforementioned violations and the amount thereof.

111. **Typicality:** Plaintiff's claims are typical of those of the Class because Plaintiff, like all members of the Class, requested and viewed prerecorded videos and games containing prerecorded videos on Defendant's Website and had their PII collected and disclosed by Defendant to third parties.

112. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class as required by Federal Rule of Civil Procedure Rule 23(a)(4). Plaintiff is an adequate representative of the Class because Plaintiff has no interests which are adverse to the interests of the members of the Class. Plaintiff is committed to the vigorous prosecution of this action and, to that end, Plaintiff has retained skilled and experienced counsel.

113. Moreover, the proposed Class can be maintained because it satisfies both Rule 23(a) and 23(b)(3) because questions of law or fact common to the Class predominate over any questions affecting only individual members and a Class Action is superior to all other available methods of the fair and efficient adjudication of the claims asserted in this action under Federal Rule of Civil Procedure 23(b)(3) because:

(a) The expense and burden of individual litigation makes it economically unfeasible for members of the Class to seek to redress their claims other than through the procedure of a class action;

(b) If separate actions were brought by individual members of the Class, the resulting duplicity of lawsuits would cause members of the Class to seek to redress their claims other than through the procedure of a class action; and

(c) Absent a class action, Defendant likely will retain the benefits of its wrongdoing, and there would be a failure of justice.

CAUSES OF ACTION

COUNT I

Violation of the Video Privacy Protection Act 18 U.S.C. § 2710, *et seq.*

114. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

115. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally-identifiable information” concerning any “consumer” to a third-party without the “informed, written consent (including through an electronic means using the Internet) of the consumer.” 18 U.S.C. § 2710.

116. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials.” Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because it engaged in the business of renting and delivering audiovisual materials—including prerecorded videos and games containing prerecorded videos that Plaintiff and the Class Members requested and/or rented on the Website and Apps—and those deliveries affect interstate or foreign commerce.

117. As defined in 18 U.S.C. § 2710(a)(1), a “consumer” means “any renter, purchaser, or subscriber of goods or services from a video tape service provider.” Plaintiff and the Class Members are “consumers” because they:

- a. Created an account with Defendant by providing at a minimum, their first and last name, IP address and email address, then purchased, requested and/or viewed audio visual materials; and/or
- b. Made a purchase from Defendant's store through Defendant's Website.

118. Defendant knowingly caused Plaintiff's and the Class Members' Personal Viewing Information, as well as the above-referenced unique identifiers, to be disclosed to third parties, such as Facebook. This information constitutes "personally identifiable information" under 18 U.S.C. § 2710(a)(3) because it identified each Plaintiff and Class member to third parties as individuals who rented or requested audiovisual materials from Defendant. This information allowed third parties, such as Facebook, to identify each Plaintiff's and Class Member's specific video viewing preferences and habits.

119. As set forth in 18 U.S.C. § 2710(b)(2)(B), "informed, written consent" must be (1) "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;" and (2) "at the election of the consumer...is either given at the time the disclosure is sought or is given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner." Defendant failed to obtain informed, written consent from Plaintiff and the Class Members under this definition.

120. Defendant was aware that the disclosures to third parties that it shared through the tracking software that it incorporated in its Website and Apps identified Plaintiff and the Class Members. Indeed, Facebook publicly touts its ability to connect PII to individual user profiles. Defendant also knew that Plaintiff's and the Class Members' Personal Viewing Information was disclosed to third parties because Defendant programmed the tracking software into the Website's and Apps' code so that third parties would receive the video titles and consumer's unique third-party identifiers when a consumer requested and/or purchased a game or

prerecorded videos on the Website or Apps. The purpose of those trackers was to obtain identifiable analytics and intelligence for Defendant about its user base, while also benefiting Facebook and other third parties, by providing them with additional data that they can leverage for their advertising, analytics and/or other services.

121. Nor were Defendant’s disclosures made in the “ordinary course of business” as the term is defined by the VPPA. In particular, the Website’s and app’s disclosures to Facebook were not necessary for “debt collection activities, order fulfillment, request processing, [or] transfer of ownership.” 18 U.S.C. § 2710(a)(2).

122. On behalf of Plaintiff and the Class Members, Plaintiff seeks declaratory relief, statutory damages of \$2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c), and reasonable attorneys’ fees and cost.

Count II
Violation of the Federal Wiretap Act
18 U.S.C. § 2710, *et seq.*
(On behalf of Plaintiff and the Class)

123. Plaintiff incorporates by reference each of the allegations contained in the foregoing paragraphs of this Complaint as though fully set forth herein.

124. The Federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. 18 U.S.C. §§ 2510 *et seq.*

125. The Wiretap Act confers a civil private right of action to “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C. § 2520(a).

126. The Wiretap Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

127. The Wiretap Act defines “contents” as “includ[ing] any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

128. The Wiretap Act defines “person” as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” 18 U.S.C. § 2510(6).

129. The Wiretap Act defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce” 18 U.S.C. § 2510(12).

130. Defendant is a person for the purposes of the Wiretap Act.

131. The software deployed by Facebook constitutes a “device or apparatus which can be used to intercept a wire, oral, or electronic communication.” 18 U.S.C. § 2510(5).

132. The confidential communications Plaintiff and members of the Class had with the Website, in the form of their PII and personal viewing history, were intercepted by Facebook, and such communications were “electronic communications” under 18 U.S.C. § 2510(12).

133. While the Wiretap Act allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not “intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. §2511(2)(d).

134. Plaintiff and the Class Members had a reasonable expectation of privacy in their electronic communications with the Website in the form of their sensitive interactions with the Website about their gambling habits in general and the specific subset of gambling categories which they are interested in. Gambling inside of one’s home is an intrinsically private activity over which a person has a reasonable expectation of privacy. In fact, gambling is considered a

vice in many religions and, due to its stigma, continues to be illegal in many states. Defendant's disclosure of Plaintiff and the Class Members' gambling activities to a third party without their consent breached their expectation of privacy and rises to the level of a common law tort of intrusion upon seclusion and public disclosure of private facts. *See* Restatement (Second) Torts § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of . . . privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

135. Furthermore, Plaintiff and the Class Members had a reasonable expectation in the privacy of their electronic communications with the Website, including the video games that they searched for, requested, or gambled on, along with their identifying information is equivalent to the expectation of privacy codified under the VPPA. As such, Defendant's use of the Tracking Tools also constitutes a tortious act under the laws of the United States.

136. Plaintiff and the Class Members reasonably expected that the Tracking Entities were not intercepting, recording, or disclosing their electronic communications with the Website.

137. Within the relevant time period, the electronic communications between Plaintiff, Class Members and the Website were intercepted by the Tracking Tools the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their private information, which includes the purpose of using such private information to develop advertising and marketing strategies.

138. Interception of Plaintiff's and the Class Members' confidential communications with the Website occur whenever a subscriber uses the search bar within the Website, and when navigating various webpages of the Website, including those containing videos.

139. At all relevant times, Defendant's conduct was knowing, willful, and intentional,

as Defendant is a sophisticated party with full knowledge regarding the functionality of the Tracking Entities and the functionality of the Tracking Tools, including that allowing the Tracking Tools to be implemented on the Website would cause the private communications of its subscribers to be shared with third parties.

140. Plaintiff and the Class Members were never asked for their consent to expose their confidential electronic communications with the Website to third parties. Indeed, such consent could not have been given as the Tracking Entities and Defendant never sought any form of consent from Plaintiff or the Class Members to intercept, record, and disclose their private communications with the Website.

141. As detailed above, the Tracking Entities' unauthorized interception, disclosure and use of Plaintiff's and the Class Members' confidential communications was only possible through the Defendant's knowing, willful, or intentional placement of the tracking tools on the Website. 18 U.S. Code § 2511(1)(a).

142. Plaintiff and members of the Class have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such, Plaintiff and members of the Class are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class Members and any profits made by Defendant as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; (2) appropriate equitable or declaratory relief; and (3) reasonable attorneys' fees and expenses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant as follows:

- a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class, and Plaintiff's Counsel as Class Counsel;

- b) For an order declaring that Defendant's conduct violates each of the statutes referenced herein;
- c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- e) For prejudgment interest on all amounts awarded;
- f) For an order of restitution and all other forms of equitable monetary relief;
- g) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 14, 2025

GUCOVSKI ROZENSHTeyN, PLLC.

By: /s/ Adrian Gucovski
Adrian Gucovski, Esq.

Adrian Gucovski
Benjamin Rozenshteyn
Nathaniel Haim Sari (*pro hac vice* forthcoming)
140 Broadway, FL 46
New York, NY 10005
Telephone: (212) 884-4230
Facsimile: (212) 884-4230
E-Mail: adrian@gr-firm.com
ben@gr-firm.com
nsari@gr-firm.com

Attorneys for Plaintiff and the Putative Class